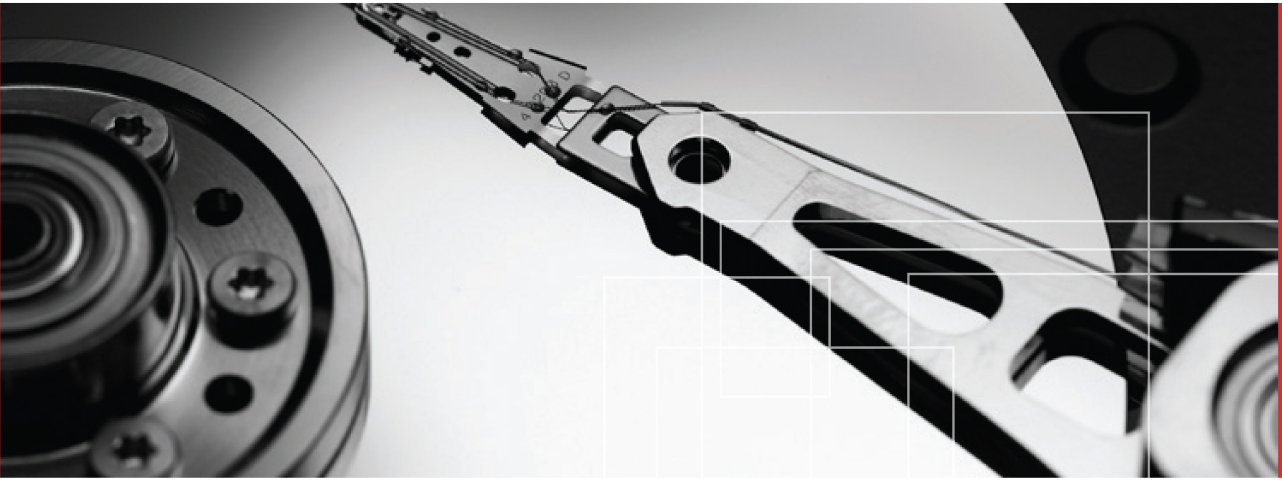
The Sleuth Kit and
Open Source Digital Forensics Conference



October 3, 2012

Automated Forensics with the Sleuth Kit Framework

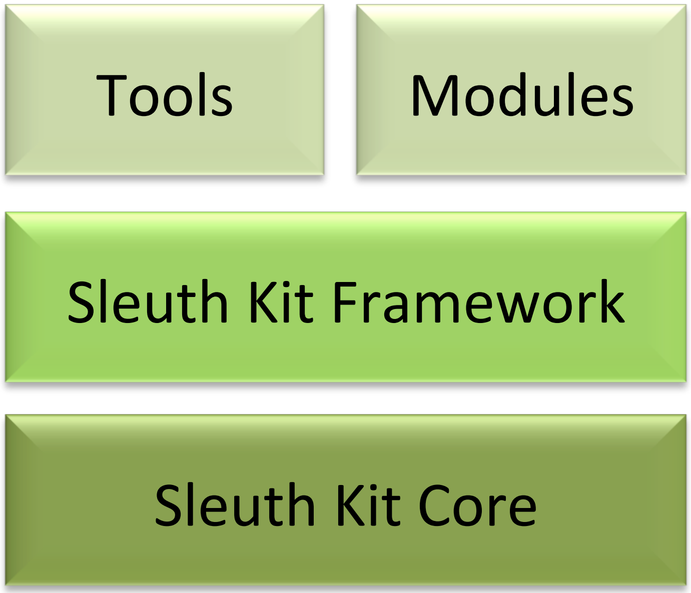
Eamonn Saunders

Principal Software Engineer, Digital Forensics

Basis Technology

What is the framework?

- Infrastructure distributed with The Sleuth Kit
- Supports development of pluggable modules
- Benefits
  - End to end solution
  - Automation
  - Simplifies module and tool development



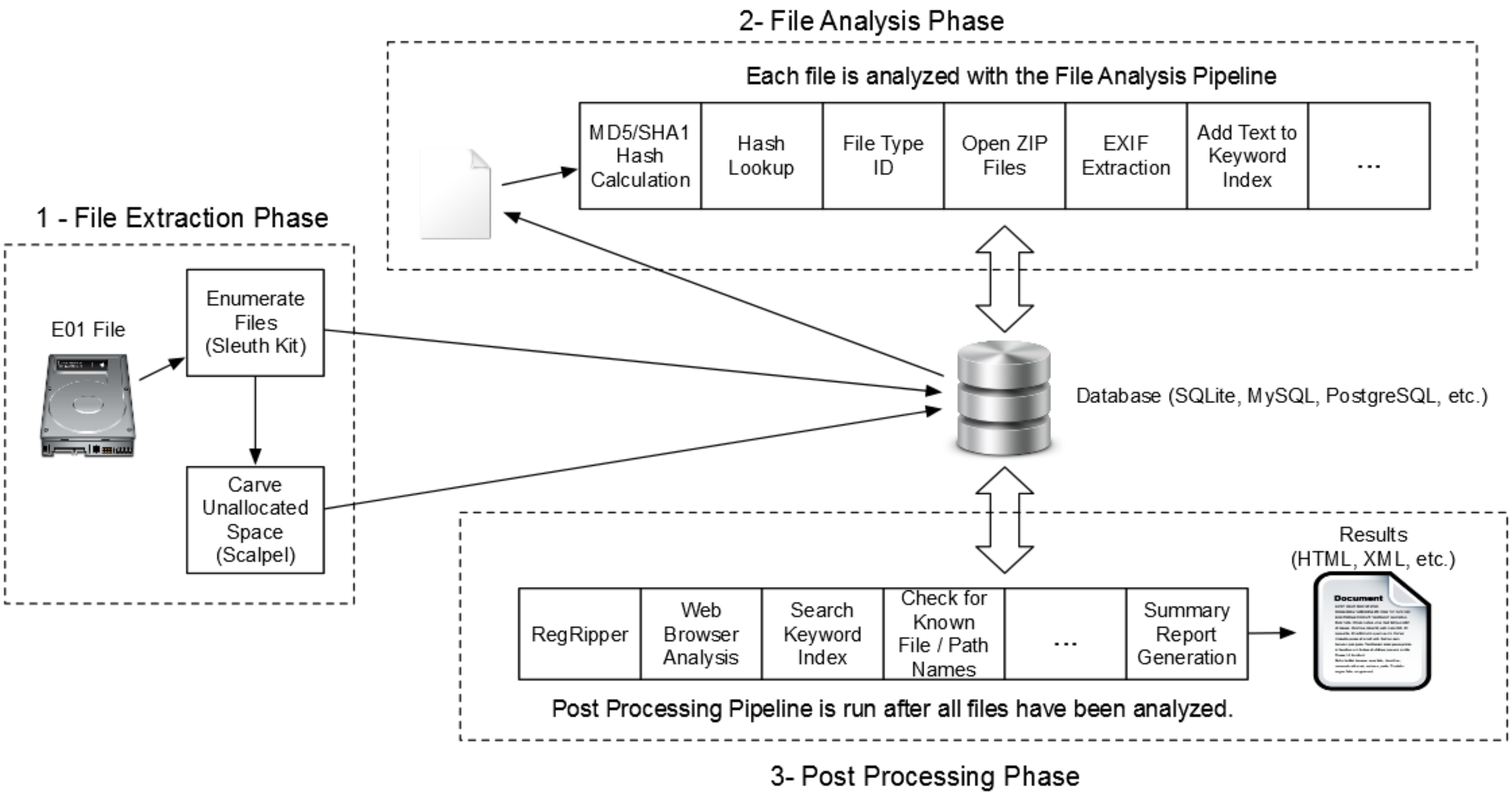
Tools

Modules

Sleuth Kit Framework

Sleuth Kit Core

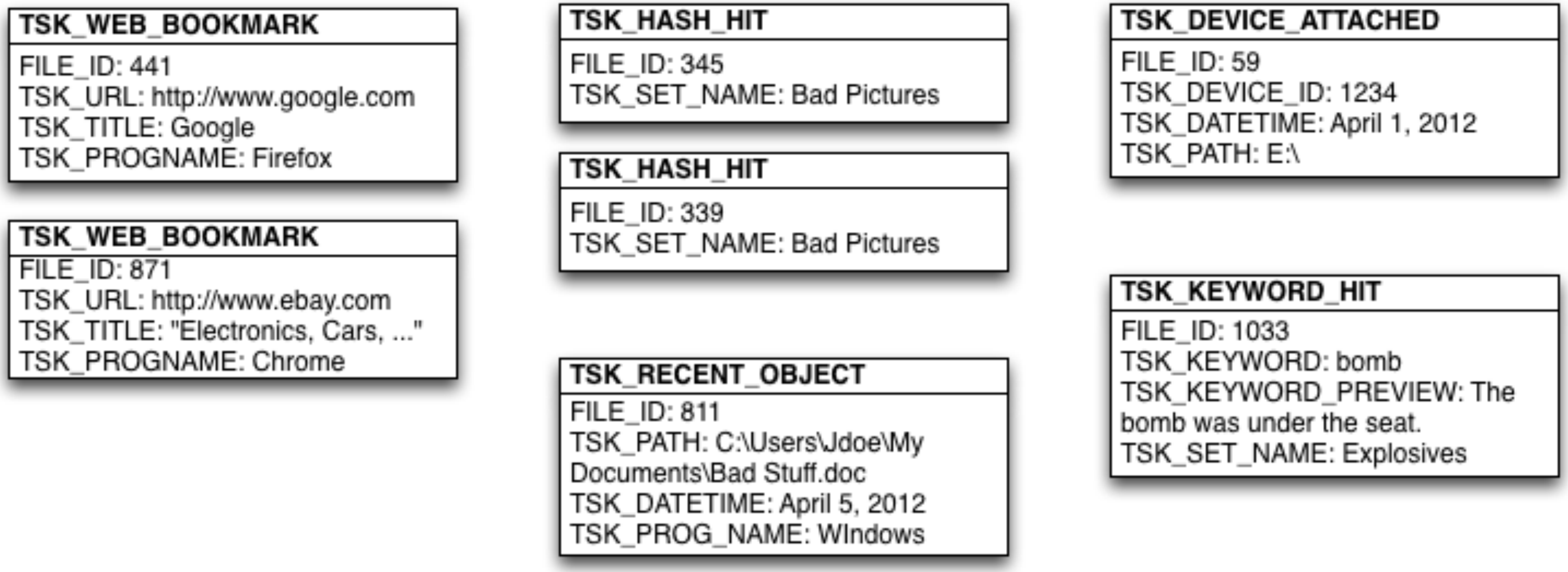
Framework Phases


2- File Analysis Phase
Each file is analyzed with the File Analysis Pipeline
MD5/SHA1 Hash Calculation
Hash Lookup
File Type ID
Open ZIP Files
EXIF Extraction
Add Text to Keyword Index
...
1 - File Extraction Phase
E01 File
Enumerate Files (Sleuth Kit)
Carve Unallocated Space (Scalpel)
Database (SQLite, MySQL, PostgreSQL, etc.)
Results (HTML, XML, etc.)
Document
RegRipper
Web Browser Analysis
Search Keyword Index
Check for Known File / Path Names
...
Summary Report Generation
Post Processing Pipeline is run after all files have been analyzed.
3- Post Processing Phase

Framework Concept: Blackboard

- Blackboard
  - Supports inter-module communication
  - Stores results generically
  - Modules can post their own results
  - Modules can read previously posted results
  - e.g. Hash calculation, lookup

Blackboard Artifacts and Attributes



TSK_WEB_BOOKMARK
FILE_ID: 441
TSK_URL: http://www.google.com
TSK_TITLE: Google
TSK_PROGNAME: Firefox

TSK_WEB_BOOKMARK
FILE_ID: 871
TSK_URL: http://www.ebay.com
TSK_TITLE: "Electronics, Cars, ..."
TSK_PROGNAME: Chrome

TSK_HASH_HIT
FILE_ID: 345
TSK_SET_NAME: Bad Pictures

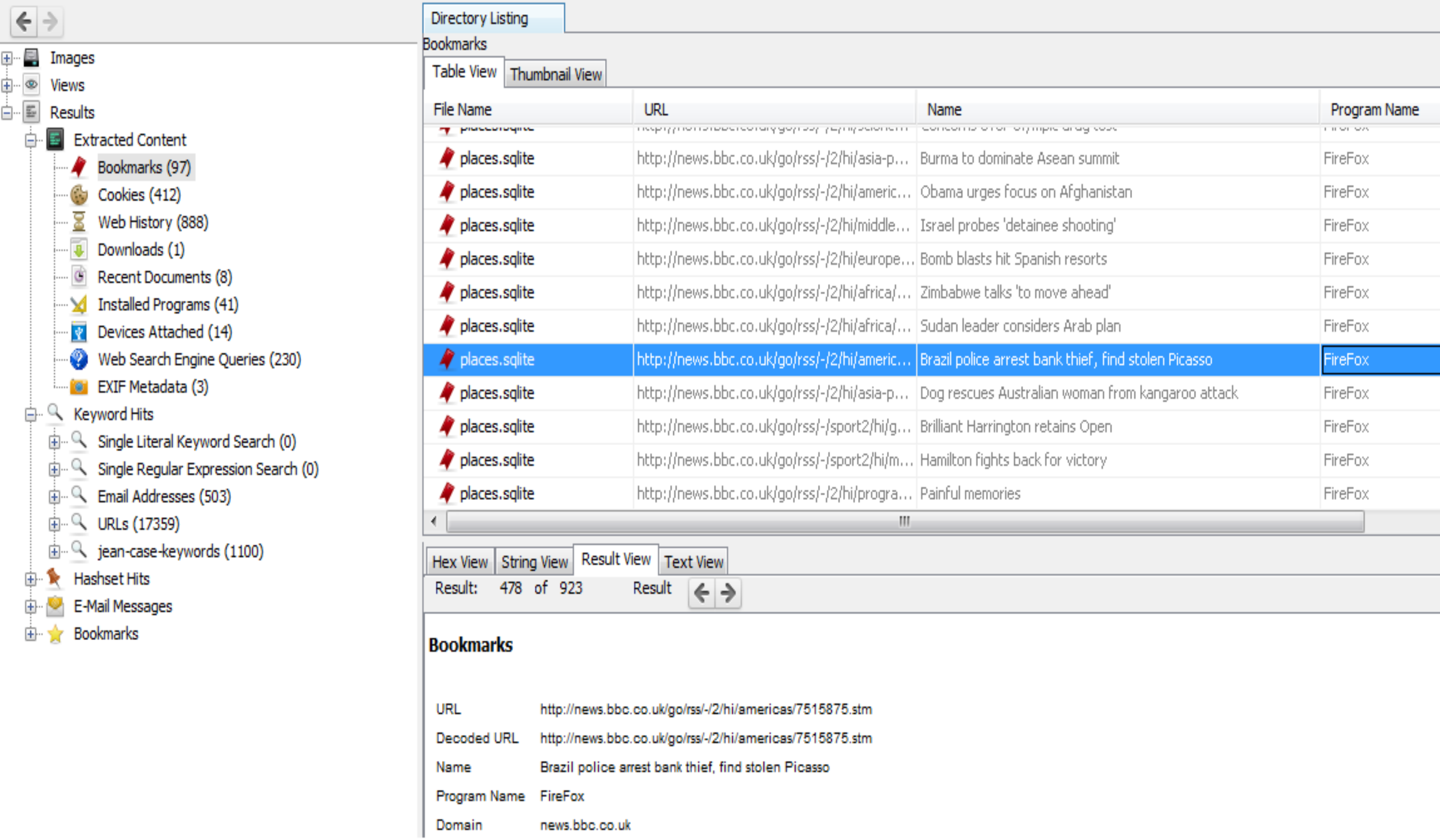
TSK_HASH_HIT
FILE_ID: 339
TSK_SET_NAME: Bad Pictures

TSK_RECENT_OBJECT
FILE_ID: 811
TSK_PATH: C:\Users\Jdoe\My Documents\Bad Stuff.doc
TSK_DATETIME: April 5, 2012
TSK_PROG_NAME: WIndows

TSK_DEVICE_ATTACHED
FILE_ID: 59
TSK_DEVICE_ID: 1234
TSK_DATETIME: April 1, 2012
TSK_PATH: E:\

TSK_KEYWORD_HIT
FILE_ID: 1033
TSK_KEYWORD: bomb
TSK_KEYWORD_PREVIEW: The bomb was under the seat.
TSK_SET_NAME: Explosives

Blackboard Bookmarks Example



- Images
- Views
- Results
  - Extracted Content
    - Bookmarks (97)
    - Cookies (412)
    - Web History (888)
    - Downloads (1)
    - Recent Documents (8)
    - Installed Programs (41)
    - Devices Attached (14)
    - Web Search Engine Queries (230)
    - EXIF Metadata (3)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
    - Email Addresses (503)
    - URLs (17359)
    - jean-case-keywords (1100)
  - Hashset Hits
  - E-Mail Messages
  - Bookmarks

File Name	URL	Name	Program Name
places.sqlite	http://news.bbc.co.uk/go/rss/-/2/hi/asia-p...	Burma to dominate Asean summit	FireFox
places.sqlite	http://news.bbc.co.uk/go/rss/-/2/hi/americ...	Obama urges focus on Afghanistan	FireFox
places.sqlite	http://news.bbc.co.uk/go/rss/-/2/hi/middle...	Israel probes 'detainee shooting'	FireFox
places.sqlite	http://news.bbc.co.uk/go/rss/-/2/hi/europe...	Bomb blasts hit Spanish resorts	FireFox
places.sqlite	http://news.bbc.co.uk/go/rss/-/2/hi/africa/...	Zimbabwe talks 'to move ahead'	FireFox
places.sqlite	http://news.bbc.co.uk/go/rss/-/2/hi/africa/...	Sudan leader considers Arab plan	FireFox
places.sqlite	http://news.bbc.co.uk/go/rss/-/2/hi/americ...	Brazil police arrest bank thief, find stolen Picasso	FireFox
places.sqlite	http://news.bbc.co.uk/go/rss/-/2/hi/asia-p...	Dog rescues Australian woman from kangaroo attack	FireFox
places.sqlite	http://news.bbc.co.uk/go/rss/-/sport2/hi/g...	Brilliant Harrington retains Open	FireFox
places.sqlite	http://news.bbc.co.uk/go/rss/-/sport2/hi/m...	Hamilton fights back for victory	FireFox
places.sqlite	http://news.bbc.co.uk/go/rss/-/2/hi/progra...	Painful memories	FireFox

Result: 478 of 923 Result

Bookmarks

URL	http://news.bbc.co.uk/go/rss/-/2/hi/americas/7515875.stm
Decoded URL	http://news.bbc.co.uk/go/rss/-/2/hi/americas/7515875.stm
Name	Brazil police arrest bank thief, find stolen Picasso
Program Name	FireFox
Domain	news.bbc.co.uk

Available Modules

Module Name	Example Use Case(s)
Hash Calculation/Hash Lookup	Find all known (e.g. NSRL) or notable files.
Entropy	Find potentially encrypted files.
File Type Identification	Find files of a particular type or identify files whose extension does not match type.
Exif Extraction	Identify location, device make/model, author information for JPEG images.
Zip Extraction	Circumvent attempts to hide data in zip files.
Interesting Files	Find Skype database files (main.db, *.dbb) or all multimedia content (*.mpg/wmv/avi etc.)
SaveInterestingFiles	Extract all multimedia content for further analysis.
RegRipper	Analyze system registry files.
SummaryReport	Present results of analysis modules.

Using the framework

- Framework is a foundation
- Incorporate framework into other tools
- tsk_analyzeimg
  - Sample implementation for testing
  - Extracts files from disk image into SQLite
  - Runs file analysis and post processing pipelines

    tsk_analyzeimg.exe C:\Images\testimage.E01

Using the framework (contd.)

- Configure modules in pipeline_config.xml

```
<?xml version="1.0" encoding="utf-8"?>
<PIPELINE_CONFIG>
 <PIPELINE type="FileAnalysis">
      <MODULE order="1" type="plugin" location=“HashCalcModule.dll"/>
      <MODULE order=“2" type="plugin" location=“HashLookup.dll"/>
 </PIPELINE>
 <PIPELINE type=“PostProcessing">
   <MODULE order="1" type="plugin" location="SummaryReport.dll"
arguments=“#OUT_DIR#\Summary.htm"/>
 </PIPELINE>
</PIPELINE_CONFIG>
```

What does a module look like?

- TskModule::Status initialize(const char * args)
  - Called when the framework loads the module
- TskModule::Status run(TskFile * pFile)
  - Called by file analysis pipeline for each file
- TskModule::Status report()
  - Called by post processing pipeline
- TskModule::Status finalize()
  - Called when the framework unloads the module

http://www.sleuthkit.org/sleuthkit/docs/framework-docs/index.html

What's next?

- We will continue to support TSK framework
- Call for developer participation
  - https://github.com/sleuthkit/sleuthkit/issues
  - Add new modules to Wiki page
    - http://wiki.sleuthkit.org/index.php?title=TSK_Framework_3rd_Party_Modules
  - More platforms: (Linux, Mac)
  - …
- Ideas and contributions are always welcome.

Thank you!

For more information:

Visit www.basistech.com

Write to conference@basistech.com

Call 617-386-2090 or 800-697-2062